Strategy Research Project

THE STRATEGIC PARADOX OF SOCIAL NETWORKS

BY

COLONEL ROBERT COTE
United States Marine Corps

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
18-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE
The Strategic Paradox of Social Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Robert Cote

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Lee Deremer
Department of Command, Leadership, & Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

During the past few decades, the world witnessed social media's climb from relative obscurity to a primary means of communication for millions of people. Mirroring their civilian counterparts, military organizations and individual service members discovered the benefits of social media services like Facebook, MySpace, LinkedIn, and Twitter. The Department of Defense (DOD) recognized social media's value as a tool for strategic communication, and even approved the private use of social media networks on government computers. But the use of social media networks presents risks for military leaders. While imposing control measures may address some concerns, a sense of irony surrounds the military's efforts to harness the productivity of social networks, while attempting to control the information published online.

15. SUBJECT TERMS
Cyber, Civil Military Relations, War and Society

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	28	

USAWC STRATEGY RESEARCH PROJECT

THE STRATEGIC PARADOX OF SOCIAL NETWORKS

by

Colonel Robert Cote
United States Marine Corps

Professor Lee Deremer
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Robert Cote

TITLE: The Strategic Paradox of Social Networks

FORMAT: Strategy Research Project

DATE: 18 March 2011 WORD COUNT: 5,028 PAGES: 28

KEY TERMS: Cyber, Civil Military Relations, War and Society

CLASSIFICATION: Unclassified

During the past few decades, the world witnessed social media's climb from relative obscurity to a primary means of communication for millions of people. Mirroring their civilian counterparts, military organizations and individual service members discovered the benefits of social media services like Facebook, MySpace, LinkedIn, and Twitter. The Department of Defense (DOD) recognized social media's value as a tool for strategic communication, and even approved the private use of social media networks on government computers.[1] But the use of social media networks presents risks for military leaders. While imposing control measures may address some concerns, a sense of irony surrounds the military's efforts to harness the productivity of social networks, while attempting to control the information published online.

THE STRATEGIC PARADOX OF SOCIAL NETWORKS

During the past few decades, the world witnessed social media's climb from relative obscurity to a primary means of communication for millions of people. Mirroring their civilian counterparts, military organizations and individual service members discovered the benefits of social media services like Facebook, MySpace, LinkedIn, and Twitter. The Department of Defense (DOD) recognized social media's value as a tool for strategic communication, and even approved the private use of social media networks on government computers.[2] But the use of social media networks presents risks for military leaders. While imposing control measures may address some concerns, a sense of irony surrounds the military's efforts to harness the productivity of social networks, while attempting to control the information published online.

The rapid evolution of social media highlights many ethical, legal, and security issues confronting the U.S. military. Conversations which once took place between individuals or inside private groups could now remain in cyberspace indefinitely. The simple act of posting information on the Internet could make users of social media victims of their own impulsive behavior or lapses in judgment. Every day, examples of embarrassing information surfaces on social media networks. Members of the military or other government organizations must guard against publishing comments or material which may violate official regulations or directives. Also, the considerable amount of open source information on social media websites elevates the vulnerability of computer networks to cyber attacks, cybercrime, or privacy violations. Additionally, social media networks offer a new means for strategic communication. This, in turn, creates new challenges for military leaders. The Internet's speed of information flow reduces

response times, especially when addressing crisis situations during today's twenty-four hour news cycle. As social media networks continue to expand, the DOD and its subordinate branches continue to refine guidelines for official and private use. However, existing ambiguities in social media networks will continue to present challenges for military leaders.

Few technological innovations are considered revolutionary. Reminiscent of the printing press, telegraph, or television, the Information Age markedly transformed the means of communication. Within a few decades, society witnessed a localized network of computers develop into a series of global connections which minimized many preexisting cultural and geographical boundaries.[3] In his book "The World is Flat: A Brief History of the 21st Century," Thomas Friedman describes this phenomenon as

> …the product of a convergence of the personal computer (which allowed every individual suddenly to become the author of his or her own content in digital form) with fiber optic cable (which suddenly allowed all those individuals to access more and more digital content around the world for next to nothing) with the rise of work flow software (which enabled individuals all over the world to collaborate on that same digital content anywhere, regardless of the distances between them).[4]

Internationally, the number of Internet users rose from 0.8 billion in 2003 to 1.8 billion in 2009 (roughly 27% of the world's population).[5] As computer-based systems became more accessible and affordable, online social networks gained recognition as a convenient means of communication. Also key was introducing Web 2.0 software, which changed the user's interaction with the Internet. How popular are online social networks? Research conducted by the Pew Internet & American Life Project into the use of social media by teens and young adults points out that online social networks are thriving.[6] Statistics gathered in May 2010 showed 95% of young adults aged 18-29, 87% of adults aged 30-49, and 78% of adults aged 50-54 used the Internet.[7] Of online

users, 73% of teens, 72% of young adults, and 40% of adults accessed social network sites; mainly Facebook, MySpace, and LinkedIn.[8] Other statistics underscore social media's cultural impact. For instance, in 2009, 1 of 8 couples married in the United States claimed to have met online.[9] And in 2010, Facebook claimed over 500 million users, which would make the social networking service the third largest "country" in the world after China and India.[10]

This technology is a powerful communication tool. For instance, many law enforcement organizations use online social networks to release media and public updates (such as "amber alerts"); to provide real time updates to criminal blotters; to post pictures of suspects; or to receive anonymous tips.[11] Undercover officers even pose as gang members on social media websites to infiltrate criminal networks.[12] Law enforcement's use of social media increases their effectiveness and improves their communication with the public.

The growth of social media networks represents a fundamental shift in the way people communicate, since Internet-based information travels faster, to a larger (or focused) audience. Consider events over fifty years ago, during the civil rights movement. In 1960, four African-American gentlemen staged a "sit in" protest at a lunch counter in Greensboro, North Carolina to publicize racial discrimination practices. News of the event spread using the principle technologies of the time: television, radio, and telephone. Within days, thousands of people were marching in solidarity across the American South. Today, online social networks complement older forms of communication. The 2009 protests in Iran and Moldova became famously known as 'twitter revolutions" after political organizers announced grievances and organized

demonstrations on social networks.[13] In fact, the impact of social networking during the Iranian protests caused the U.S. State Department to ask that Twitter delay their regularly scheduled maintenance, so to not interrupt coverage.[14] During the 2011 demonstrations in Egypt, over 80,000 people signed up on Facebook to join protests in Cairo.[15] Imagine the impact on the protests in 1960 with today's social networks.

The DOD recognizes social networks represent an important means for strategic communication and information management. Senior U.S. military officials comment regularly on social networks about current events or attempt to focus attention towards particular areas of interest.[16] A majority of military units, organizations, and affiliations sponsor individual social network sites, which improve older methods of "spreading the word" like phone trees or newsletters. Social media's information flow enhances communication even after someone's transferred or left active duty. Separate websites also exist that promote membership based on commonalities like school, service culture, or occupational specialty.

One drawback with social networks concerns the protection of individual privacy. Facebook, for example, has faced strong criticism for sharing private user information with marketing agencies and commercial websites.[17] In 2007, Facebook launched an application called Beacon, which tracked individual online purchases, then forwarded sales information to other Facebook accounts. But some purchases are best left anonymous. A few years ago, a young woman found out about an impending marriage proposal after receiving a message from Facebook highlighting her boyfriend's purchase of a diamond engagement ring.[18] And recently, two members of Congress questioned Facebook's CEO about the "recent announcement - and postponement - of

a plan to make the addresses and cell phone numbers of its users available to third-party websites and application developers…"[19] The ease of getting information such as birthdates, addresses, phone numbers, or names of relatives from social media networks is alarming. With over 150 million users in the United States and more than 500 million users worldwide, Facebook's revenue this year could reach 1.4 billion dollars.[20] Companies profit from gathering personal information; when users post information online, they can unknowingly contribute third-party data to marketing profiles.[21] Companies planning to target a specific group of consumers can use this information to build an effective marketing strategy.

The popularity of social media networks increased the amount of personal information on the Internet.[22] Some material can cause long-lasting effects. For example, a recent Career Builder survey found the number of civilian employers who used social networking sites as a screening tool for job applicants rose from 22% in 2008 to 45% in 2009.[23] This particular survey also found 35% of employers disqualified an interviewee after discovering information such as poor communication skills, inappropriate or disparaging comments, or suggestive photographs on a social networking site.[24]

Even nonusers of social media are vulnerable to information published online by third parties. In 2009, a news story reported the wife of the then-incoming head of Britain's Secret Intelligence Service was posting personal information on her Facebook page.[25] Since she did not enable any privacy protection measures, her information was viewable by anyone owning a Facebook account within their local network.[26] The information she posted online-including addresses, children's activities, and family

pictures-could be easily exploited by terrorists or other intelligence organizations.[27] This example shows how social media networks even impact nonusers.

Awareness of personal information on social networking websites can provide valuable insight to military leaders about their personnel. But is it ethical to use social media as an investigative tool? Take, for example, someone experiencing personal problems or suspected of misconduct. When is it acceptable to screen someone's personal websites for information? Where does the final authority rest when deciding whether or not to search these sites? On one hand, some may argue that using the Internet to collect third-party information is no different from older means of gathering information. On the other hand, private information which would not normally factor into decision making - such as religion, sexual orientation, or other content - could become an impediment during an investigation.

Social network sites offer "treasure troves" of personal information.[28] However, this information is often inaccurate, misinterpreted, or taken out of context.[29] Echoing the Career Builder survey, some military guidelines now warn that user information on social networking websites can affect background investigations or security clearances.[30]

The growing availability of open source information on the Internet highlights several legal and ethical considerations. Military leaders should try to define clear boundaries addressing the use of social networks as a screening tool; but each user bears responsibility in deciding what material appears online.

Another concern of social networking involves the prospective blurring of lines in professional and private relationships. Social media websites promote a relaxed

atmosphere, which may present a perception of partiality or fraternization, and could undermine unit discipline and morale. As the famous fable teller Aesop once wrote, "You are judged by the company you keep."[31] Although Aesop lived in ancient Greece, his quote still resonates today. Social media has not changed the foundations of military professionalism.

One way to evaluate the military's effectiveness using social media is by measuring the "fan count," which reflects the popularity of a specific site. In March 2010, Janson Communications conducted a 'Military Facebook Study" to research "trends, themes, and commonalities between Facebook users and owners."[32] As part of their study, Janson ranked the top military organizational pages and found the United States Marine Corps claimed the most fans (241,515), followed by the National Guard (224,623) and the U.S. Army (152,958).[33] A key point from the Janson study states the military can use social networks as a strategic communication tool to effectively address a large audience.[34] For example, when the DOD wished to promote awareness about the dangers of synthetic marijuana, its Drug Demand Reduction Program circulated informational videos on social media networks.[35] Also, the U.S. Air Force produced a video series entitled "Portraits of Courage," which promotes inspirational stories of individual Airmen, and appears on several social media websites.[36] Readers can forward this information and quickly improve a story's circulation.

Social networking websites provide an effective means for strategic communication. One concern, however, is authenticity: modest users may find it difficult to distinguish an officially approved site from an imposter. Janson's research noted that "many military Facebook pages are not clearly marked as "official" and can

be confused with unofficial or "clone" pages that look like government sponsored pages but may contain inaccurate and inappropriate content."[37] One predicament lies with the ever-present possibility that unofficial sites will contain threads discussing, for instance, politically sensitive topics such as the recent repeal of the "don't ask, don't tell" policy. Some readers may even mistake inappropriate comments as a sanctioned statement. To confuse matters even further, individuals identifying themselves with the military (often using graphics to associate with a particular service, unit, or specialty) can join the debate and contribute inflammatory remarks or inappropriate comments. On the official sites, Janson's study recommends the military "manage the page and ensure inappropriate posts are quickly identified and deleted by the administrator."[38]

Service members discussing political subjects on social networking sites can quickly attract negative attention. In March 2010, Marine Corps Sergeant Gary Stein decided to express his concerns with President Obama's domestic agenda. Alarmed over the Obama Administration's quest for health care reform legislation, Stein, identifying himself as an active duty U.S. Marine, started a Facebook page named "Armed Forces for Tea Party Patriots."[39] The website quickly grew popular; Stein's association with the Marine Corps on his Facebook website lent a perception of authenticity to his message. Soon after, the television channel MSNBC invited Stein to appear on their news program to discuss his views on healthcare.[40] But before the interview took place, Stein's chain of command advised him to review existing DOD policies on political activities.[41] One of these directives clearly states that active duty service members may not "participate in any radio, television, or other program or group discussion as an advocate for or against a partisan political party, candidate, or

cause."[42] After his reprimand, Stein prudently canceled the television interview and shut down the offending website.[43] But Stein refused to remain away from the public eye. Displaying his unfamiliarity with the DOD directives, not to mention the Uniform Code of Military Justice, Stein stated that "There's this illusion that when we sign our contract and voluntarily commit, that we lose our right to speak out."[44] Not surprisingly, Stein attracted the attention of the American Civil Liberties Union (ACLU), which supports the individual's right to "discuss and critique the government's policies and conduct."[45] Referring to Stein, an ACLU spokesman added, "We think service members ought to be entitled to virtually the same free speech rights as civilians with very limited exceptions for the necessity of combat."[46] Stein later opened another Facebook page, also named "Armed Forces Tea Party Patriots," which currently lists over 17,000 fans.[47] This time, though, Stein did not associate himself with the Marine Corps.

Despite the opinion shared by the ACLU and other civil liberty groups that military personnel share the same 1st Amendment rights as their civilian counterparts "with very limited exceptions," the Uniform Code of Military Justice (UCMJ) provides clear guidance on permissible speech for military service members.[48] For example, Article 88 of the UCMJ cautions officers against using "contemptuous words against the President, the Vice President, Congress, the Secretary of Defense" or other prominent members of Federal and State governments.[49] Article 89 defines disrespect toward a senior commissioned officer as "acts or language, however expressed, and it is immaterial whether they refer to the superior as an officer or as a private individual. Disrespect by words may be conveyed by abusive epithets or other contemptuous or denunciatory language. Truth is no defense."[50] Information published in cyberspace,

even if only intended for a select audience, remains in the public domain indefinitely. Military personnel are well-known for voicing their opinions; only now, statements can remain in cyberspace indefinitely.

At least the DOD has legal authority over personnel serving either on active duty or in a reserve status. But those who are not under the DOD's jurisdiction can also publish sensitive information on the Internet. For instance, during a squadron's recent redeployment from Afghanistan, this author received the best updates by reading a Facebook site managed by the spouse of the squadron's Commanding Officer. In this case, the spouse received updates over the phone from her husband, and posted the information online. This incident, although minor, demonstrates how easily sensitive information appears over the Internet.

Journalists embedded with military units also effectively use social networks, quickly relaying their experiences over the Internet to a large audience. One popular "blogger" is Michael Yon, who began writing after serving in the U.S. Army's Special Forces. His popularity- a Facebook page boasts over 42,500 fans-provides evidence of his credibility with readers.[51] Yon's straightforwardness was clear in 2010, while embedded in Afghanistan with the International Security Assistance Force (ISAF). Writing about General Stanley McChyrstal, then assigned as Commander of ISAF and U.S. Forces Afghanistan, Yon stated General McChyrstal was "…a great killer but this war is over his head. He must be watched…"[52] After publishing more disparaging comments, IASF Headquarters dismissed Yon, who referred to his removal as a "…very bad sign. Sends chills that McChrystal himself thinks we are losing the war. McChrystal has a history of covering up. This causes concern that McChrystal might be

misleading SecDef and President. Are they getting the facts?"[53] Following General McChrystal's infamous interview with Rolling Stone magazine, Yon continued comment online, stating that "…if a Colonel under General McChrystal's chain of command publicly dismissed General McChrystal in a major magazine, McChrystal would be forced to fire him or appear weak and not in control."[54] Although Yon's comments did not influence the specific events surrounding General McChrystal's dismissal, his opinions reach thousands of readers, many of whom currently serve on active duty. Although Yon does not appear to view the military with malice, his potential for shaping opinions should not be discounted.

Other journalists portray a negative bias against the military. Zoriah Miller publishes his comments and photos on several websites, including a personal blog and Facebook page which detail recent conflicts in Afghanistan and Gaza, famine in Kenya, and Gulf of Mexico oil spill. Miller earned notoriety in August 2008, after he posted graphic photos detailing the aftereffects of a suicide bombing in Iraq.[55] Among the causalities were dozens of Iraqi civilians and several U.S. Marines, including a battalion commander. After refusing to remove the provocative pictures, the Marines removed Miller from their location. In November 2008, Miller published dozens of images which he claims were photographed inside U.S. camps in Iraq and Kuwait. These photographs depict derogatory, profanity-laced graffiti directed at then-President Bush and the U.S. presence in Iraq. Michael Yon and Zoriah Miller demonstrate how social media works outside DOD rules and regulations, yet remains influential and capable of influencing public opinion.

During the Abu Ghraib incident, U.S. officials maintained time to build a public relations strategy before the release of graphic photos depicting mistreatment Iraqi detainees. In fact, military officials provided media outlets with details of its investigation, even conducting preliminary interviews with CBS News before publishing the incriminating images. With social media, inflammatory material can appear overnight, create a following of interested readers, and compel officials into addressing the media earlier than desired. In August 2010, the Israeli news source Haaretz.com published a story about a former Israeli Defense Soldier who posted "pictures posing next to blindfold [sic] Palestinian prisoners on Facebook."[56] These images quickly circulated across the Internet and were picked up by other bloggers and web sites.[57] An Israeli Non Government Organization (NGO) posted other pictures on Facebook showing "…an IDF soldier pointing a gun at a blindfolded man… a soldier squatting in a kitchen where two women donning hijabs are cooking" and "a soldier spraying graffiti…in Hebrew."[58] This particular NGO, which calls itself "Breaking the Silence," aims to "…portray a different and grim picture of questionable orders in many areas regarding Palestinian civilians."[59] Supporters of the beleaguered soldier started their own Facebook page, adding explicit photos showing other Israeli soldiers engaged in provocative behavior, and even posting pictures from Abu Ghraib, with a caption reading: "This is what Americans do to Iraqi soldiers - Guys, can we really compare?!! [The soldier] only took a picture next to them - she didn't humiliate them or anything."[60] Breaking news on social media can catch military officials by surprise and quickly spiral out of control.

U.S. officials also enjoyed ample time to respond to recent allegations against soldiers operating in Afghanistan while assigned to the 5th Stryker Combat Brigade. During an early inquiry, investigators desperately searched for digital photographs taken in Afghanistan which allegedly portrayed images showing the commission of war crimes.[61] If photos from this incident or Abu Ghraib had first appeared online, military officials would have had no chance to preemptively address the media and try to control the public message. Working from a reactive position, the resulting media frenzy and public outcry would have undoubtedly caused even greater damage to the U.S., its policy towards Iraq and Afghanistan, and the public opinion of the military profession than the original incidents.

Also, documented cases show military operations were compromised after sensitive information appeared on social networking sites. In March 2010, stories surfaced reporting the Israeli army canceled a mission after a soldier “disclosed the name of the combat unit, the place of the operation and the time it will take place" on his Facebook site.[62] The soldier wrote, "On Wednesday we clean up Qatanah [a village near Ramallah], and on Thursday, god willing, we come home."[63] Fortunately, the soldier’s chain of command discovered the security breach before it was too late. But military can’t rely on watchdogs to supervise all the information published on the Internet. Adversaries also browse social media networks, and can piece together information which may have serious ramifications for U.S. national security.

In December 2010, several U.S. financial websites experienced “denial of service” cyber attacks from supporters of Julian Assange, following Assange’s arrest for his role in the release of thousands of classified U.S. State Department documents.[64]

This incident offers further proof of the vulnerability of computer networks to security breaches; social networking sites are subject to these same threats. Hackers are engaging in increasingly sophisticated attacks designed to illegally gain personal information such as passwords, or find an association with targeted individuals or groups. For example, social engineering attacks play "psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system."[65] Users of social network sites also risk "downloading viruses that could work in a similar way that an email virus works, sometimes immediately attacking user's system - at other times lurking for months before any damage is noticeable."[66]

The 2010 U.S. National Security Strategy warns that "…cyber security threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[67] Increased reliance on computer networks present added opportunities for adversaries to target national interests "…directly or indirectly with criminal activity, terrorism, or armed aggression on a transnational scale with relative ease and with little cost."[68] China, for instance, "…conducts perception management operations here in the United States in order to manipulate American and international opinion and to strengthen its position vis-à-vis the United States, and it probes the cyber defenses of important military and economic centers for their vulnerabilities."[69] The security vulnerabilities of social networking systems provide an additional portal for cyber attacks.

Intelligence services closer to home are also looking for new ways to analyze and exploit open source information on the Internet, including social networks. The Central Intelligence Agency, recognizing that private sector companies consistently

outpace the government in technological innovations, created the non-profit corporation In-Q-Tel in 1999 in an effort to maintain a competitive edge in cyber technology.[70] As the only federally funded venture capital firm in the United States, In-Q-Tel invests in high tech companies, supporting private research can provide the most up to date technology to serve U.S. intelligence assets.[71]

As recently as 2009, the DOD banned private use of social network sites on government computers due to the "…particularly high risk due to information exposure, user generated content and targeting by adversaries."[72] But only one year later, the DOD rescinded its ban, deciding instead to allow "…limited personal use of Federal Government resources…on a non-interference basis. When accessing Internet-based capabilities using federal government resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures…and shall not represent the policies or official position of the Department of Defense."[73] This decision was likely welcomed by junior personnel, and preserved access to social networking sites for deployed service members. But there are two concerns with this decision. First, allowing access to personal social networking accounts at the workplace is unproductive for both the user, who is invited to spend time browsing the internet, and the supervisors, who are forced to devote more time managing added distractions while trying to conduct business as usual. The second concern surrounds the increased vulnerability of government networks to cyber attacks. This added exposure raises the chances of a cyber attack similar to one in 2008, when a military laptop in the Middle East was infected by a "…rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary."[74] There are

plenty of other ways to access social media sites without causing avoidable distraction at work and subjecting government networks to unnecessary risk.

The most significant risk associated with online social networking is the threat from either rogue hackers acting for independent gain or more sophisticated groups seeking a competitive advantage against the United States or its allies. The current U.S. National Security Strategy notes America's dependence on computer networks, recognizes the threat of cyber warfare, and identifies the need to secure cyberspace to defend against future cyber attacks.[75] To counter these threats, the United States should continue to develop a strong cyber policy in partnership with private sectors and U.S. allies. In November 2010, the U.S. Department of Homeland Security signed a memorandum of understanding with U.S. Cyber Command to enhance cooperation between agencies and improve overall cyber defense capabilities.[76] Collaborative efforts such as these represent a start, but more cooperative domestic and international partnerships are needed for a cohesive cyber strategy. Coordination across all spectrums is critical to navigating the myriad legislative, ethical, and international issues that will arise when facing varying degrees of cyber attacks.

Social media networks continue to draw attention to First Amendment debates over freedom of speech. Increasingly, managers of social media websites are showing their receptiveness to concerns about controversial material posted online. After U.S. Congressman Anthony Weiner objected to videos posted by Islamic cleric Anwar al-Awlaki, You Tube removed the material from their website. Awlaki, who currently resides in Yemen, posted the videos to recruit al-Qaeda terrorists.[77] YouTube officials said they would remove any material encouraging "…dangerous or illegal activities such

as bomb making, hate speech, and incitement to commit violent acts."[78] Hopefully, this incident signals an increasing willingness of social networks to cooperate with military officials when questionable material is posted online.

Current DOD guidance on social networks is informative, but contains generic language which appears to delegate a large part of the responsibility for training and supervision to the lower echelons of command. Separate guidelines established by separate branches of the military seem to follow the example set by DOD. As social media networks become further entrenched within public and private infrastructure, the hazards associated with its use deserve more than simple lip service. First, legal definitions should be clarified. Service members should understand their right to privacy; their responsibility for content posted online; the regulations concerning fraternization; and other actions which could be viewed as service discrediting or counter to good order and discipline. DOD rules and regulations should synchronize with today's technology.

Second, the U.S. military should adopt more proactive measures to counter the speed at which information travels across the Internet-which often forces a reactive response, which is not preferred. During the time spent drafting a media message, a story can quickly "go viral" in today's news cycle. The longer it takes to release an effective message out, the less impact it will have with the reader. Often, official military spokespersons are the first responders; but their rank and title often lend the impression of giving the "party line."

One way to improve the military's response time involves a compromise that balances the risks associated with social media while empowering military personnel

with this technology. The existence of a “zero defects” mindset reduces the likelihood of participation for fear of reprimand. Encouraging personnel to respond using their rank or professional credentials as a means of credibility is one way to increase the military’s reactiveness. The public understands, and often appreciates the frankness of junior personnel appearing on the news. The U.S. military already embraces the “strategic corporal” concept during combat operations; there is no reason this same mind-set can’t apply to social media.

Third, the military should limit private use of social media networks on government computers. Official use aside, private use of social media on government computers should only occur on a case-by-case basis, like during deployments or when other computer networks are not available. Given the various personal means available access social media networks, the risk outweighs the benefit when extending use to government computers, and further exposing networks to cyber security threats.

Finally, social media training must occur early and often throughout one’s military career. With training time already at a premium, introducing another block of interpersonal instructional training is likely to meet with skepticism. Done creatively, social media education can take place in conjunction with other training like ethics, public affairs, or military professionalism. Plenty of guidance exists within the DOD; each branch of military service, and many subordinate commands, publishes separate guidelines outlining the importance of protecting Operations Security (OPSEC), exercising good judgment, and using disclaimers when expressing personal views.

The ascendance of online social networks from anonymity to cultural mainstay is nothing short of extraordinary. Paralleling the public’s acceptance of social media, men

and women serving in the armed forces discovered that social networks could lessen the stress incurred by their nomadic and often austere lifestyles. The DOD, with its subordinate military elements, discovered social media's value as a communication tool. Over time, social media changed from a "peak of inflated expectations" to a "plateau of productivity."[79] In other words, society continues to resolve the freedoms of the Internet against existing ethics, laws, and regulations. For the DOD and the military, the paradox lies with its limited control over the content of information posted online. The challenges facing military leaders include protecting operational security, preserving good order and discipline, managing strategic communication, and defending against cyber attacks. Despite its increasing influence on society, military leaders must understand the limits of social media's to benefit fully from this technology.

Endnotes

[1] Deputy Secretary of Defense, "Directive-Type Memorandum (DTM) 09-26 – Responsible and Effective Use of Internet-based Capabilities," February 25, 2010, http://www.defense.gov/NEWS/DTM%2009-026.pdf (accessed October 17, 2010).

[2] Deputy Secretary of Defense, "Directive-Type Memorandum (DTM) 09-26 – Responsible and Effective Use of Internet-based Capabilities," February 25, 2010, http://www.defense.gov/NEWS/DTM%2009-026.pdf (accessed October 17, 2010).

[3] Bill Gates, "Shaping the Internet Age," December 2000, http://www.microsoft.com/presspass/exec/billg/writing/shapingtheinternet.mspx (accessed October 10, 2010).

[4] Thomas L. Friedman, *The World is Flat: A Brief History of the 21st Century* (New York: Ferrar, Straus and Giroux, 2006), 10-1.

[5] International Telecommunications Union, "ICT Indicators DataBase," July 2010, http://www.itu.int/ITU-D/ict/statistics/index.html (accessed October10, 2010).

[6] Pew Internet and American Life Project, "Who's Online," May 2010, http://www.pewinternet.org/Static-Pages/Trend-Data/Whos-Online.aspx (accessed October 10, 2010).

[7] Ibid.

[8] Amanda Lenhart et al., "Social Media & Mobile Internet Use Among Teens and Young Adults," February 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx (accessed October 10, 2010).

[9] Samantha Murphy, "Social Media: Huge, and Here to Stay," July 28, 2010, http://www.technewsdaily.com/social-media-huge-and-here-to-stay-0927 (accessed December 12, 2010).

[10] Ibid.

[11] Lon Cohen, "6 Ways Law Enforcement Uses Social Media to Fight Crime," March 17, 2010, http://mashable.com/2010/03/17/law-enforcement-social-media (accessed December 12, 2010).

[12] Ibid.

[13] Malcolm Gladwell, "Small Change: Why the Revolution will not be Tweeted," *The New Yorker*, October 4, 2010, 42.

[14] Ibid.

[15] Lori Kozlowski, "Social Media and Revolution: Egypt's Protests Mimics Those in Tunisia," January 25, 2011, http://latimesblogs.latimes.com/chatter/2011/01/protests-egypt-protests-mimic-those-in-tunisia.html (accessed 1 February 2011).

[16] For example, refer to Admiral Mike Mullen's comments on http://twitter.com/thejointstaff.

[17] Douglass A. MacIntyre, "Half of Social Network Users Fear Privacy Issues," July 16, 2010, http://247wallst.com/2010/07/16/half-of-social-network-users-fear-privacy-issues (accessed December 12, 2010).

[18] Ellen Nakashima, "Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy," November 30, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html (accessed March 17, 2011).

[19] Rebecca Stewart, "Congress Calls Out Facebook," February 4, 2011, accessed from the CNN homepage at http://politicalticker.blogs.cnn.com/2011/02/04/congress-calls-out-facebook (accessed on February 13, 2011).

[20] Sara Forden, "Facebook Seeks Friends in Washington, D.C., as Privacy Concerns Mount," December 6, 2010, linked from the Seattle Times at http://seattletimes.nwsource.com/html/businesstechnology/ 2013598715_facebook06.html (accessed December 12, 2010).

[21] "Privacy Risks for Users of Social Network Sites," September 25, 2008, http://privacyinsocialnetworksites.wordpress.com (accessed December 12, 2010).

[22] Brendan Collins, "Privacy and Security Issues in Social Networking," October 3, 2008, http://www.fastcompany.com/articles/2008/10/social-networking-security.html (accessed December 12, 2010).

[23] Rosemary Haefner, “More Employers Screening Candidates via Social Networking Sites: Five Tips for Creating a Positive Online Image,” June 10, 2009, linked from the CareerBuilder.com website at http://www.careerbuilder.com/Article/CB-1337- (accessed February 16, 2011).

[24] Ibid.

[25] Michael Evan, “Wife of Sir John Sawers, the Future Head of MI6, in Facebook Security Alert,” July 6, 2009, linked from the Sunday Times homepage at http://technology.timesonline.co.uk/tol/news/tech_and_web/article6644199.ece (accessed February 16, 2011).

[26] Ibid.

[27] Ibid.

[28] Christa Richer Cook, Esq., “Social Networking Sites: Savvy Screening Tool or Legal Trap?” June 17, 2010, linked from the New York Labor and Employment Law Report at http://www.nylaborandemploymentlawreport.com/2010/06/articles/employee-privacy/social-networking-sites-savvy-screening-tool-or-legal-trap (accessed December 12, 2010).

[29] Ibid.

[30] United States Marine Corps, “Social Media Standard Operating Procedures,” linked from the U.S. Marine Corps webpage at http://www.marines.mil/usmc/Pages/SocialMediaGuidelines.aspx (accessed December 12, 2010).

[31] Aesop's Fables Translated by George Fyler Townsend, “The Ass and His Purchaser,” http://ancienthistory.about.com/library/bl/bl_aesop_ass_purchaser.htm (accessed March 5, 2010).

[32] Janson Communications, “Military Facebook Study,” March 2010, http://www.jansoncom.com (accessed October 10, 2010), i.

[33] Ibid., 13.

[34] By March 2011the Marine Corps homepage claimed over 1 million fans, a significant increase from the findings of the Janson Communications survey.

[35] Andrew Tilghman, “Pentagon Launches Anti-Spice Campaign,” October 14, 2010, http://www.airforcetimes.com/news/2010/10/military-spice-pentagon-risks-101410w/ (accessed 16 October, 2010).

[36] Amaani Lyle, “Portraits in Courage' Vol. V highlights Air Force heroes,” December 10, 2010, linked from the U.S. Air Force website at http://www.af.mil/news/story.asp?id=123234452 (accessed December 12, 2010).

[37] Janson Communications, “Military Facebook Study,” 4.

[38] Ibid., 15.

[39] Jeanette Steele, “Pendleton Marine Back on Facebook,” San Diego Union-Tribune, April 14, 2010, http://www.signonsandiego.com/news/2010/apr/14/ bn14steinfolo (accessed October 3, 2010).

[40] The Associated Press, “Marine’s Anti-Obama Facebook Comments Fuel Debate,” April 14, 2010, linked from The San Diego Union Tribune homepage at http://www.signonsandiego.com/news/2010/apr/14/marines-anti-obama-facebook-comments-fuel-debate (accessed October 3, 2010).

[41] Ibid.

[42] Department of Defense Directive 134410, “Political Activities by Members of the Armed Forces,” February 19, 2008, http://www.dtic.mil/whs/directives (accessed October 11, 2010).

[43] Jeanette Steele, “Pendleton Marine Back on Facebook.”

[44] The Associated Press, “Marine’s anti-Obama Facebook Comments Fuel Debate,” April 14, 2010, linked from *The San Diego Union Tribune* homepage at http://www.signonsandiego.com/news/2010/apr/14/marines-anti-obama-facebook-comments-fuel-debate/ (accessed October 3, 2010).

[45] The Associated Press, “Marine back on Facebook After Fueling Debate,” April 15, 2010, linked from *The San Diego Union Tribune* homepage at http://www.signonsandiego.com/ news/2010/apr/15/marine-back-on-facebook-after-fueling-debate (accessed October 3, 2010).

[46] Steele, “Pendleton Marine Back on Facebook.”

[47] Information acquired from https://www.facebook.com/ group.php?v=wall&gid=111227655575539 (accessed March 5, 2011).

[48] Jeanette Steele, “Pendleton Marine Back on Facebook.”

[49] Manual for Courts-Martial, United States (2008 ed.), IV-16.

[50] Ibid., IV-18.

[51] Information acquired from http://www.facebook.com/MichaelYonFanPage (accessed March, 5, 2011).

[52] Greg Pollowitz, “Michael Yon On General McChrystal: ‘This War Is Above His Head,’” April 15, 2010 linked from the Nation Review Online homepage at http://www.nationalreview.com/the-feed/3990/michael-yon-general-mcchrystal-war-above-his-head (accessed February 17, 2011).

[53] Michael Yon, April 15, 2010, http://www.facebook.com/ MichaelYonFanPage?v=wall&story_fbid=112864595402158 (accessed March 5, 2010).

[54] Kay B. Day, “Michael Yon’s Criticism of McChrystal Deemed Prophetic,” June 22, 2010, linked from the US Report at http://www.theusreport.com/the-us-report/2010/6/22/ michael-yons-criticism-of-mcchrystal-deemed-prophetic.html (accessed December 12, 2010).

[55] National Public Radio, “Photojournalist Disembedded After Posting Graphic Images,” August 4, 2008, linked from the NPR website at http://www.npr.org/templates/story/story.php?storyId=93267660 (accessed March 5, 2011).

[56] Haaretz Service, “IDF Soldier Posts Images of Blindfolded Palestinians on Facebook, From ‘Best Time of My Life,’” August 16, 2010, http://www.haaretz.com/news/national/idf-soldier-posts-images-of-blindfolded-palestinians-on-facebook-from-best-time-of-my-life-1.308402 (accessed October 17, 2010).

[57] Ibid.

[58] Lahav Harkov, “New Provocative Photos of IDF soldiers on Facebook,” October 25, 2010, linked from the *Jerusalem Post* at http://www.jpost.com/Israel/Article.aspx?id=192607 (accessed December 12, 2010).

[59] Ibid.

[60] Lahav Harkov, “Facebook Flooded With Photos of Detainees,” August 18, 2010, linked from the *Jerusalem Post* at http://www.jpost.com/Israel/Article.aspx?id=185147 (accessed December 12, 2010).

[61] Craig Whitlock, “Grisly Allegations in War-Crimes Probe of Army Staff Sgt. Calvin Gibbs,” The Washington Post, September 29, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/29/AR2010092904137.html (accessed October 17, 2010).

[62] Thomas E. Ricks, “You Can’t Make This Stuff Up, pt. 11,555,” March 3, 2010, http://ricks.foreignpolicy.com/posts/2010/03/03/you_can_t_make_this_stuff_up_pt_11555 (accessed October 17, 2010).

[63] Ibid.

[64] Sonja Ryst, “Cyber Attacks Hit Companies That Cut Ties With WikiLeaks,” December 13, 2010, http://www.businessinsurance.com/article/20101212/ISSUE01/312129984 (accessed December 12, 2010).

[65] Sarah Granger, “Social Engineering Fundamentals, Part I: Hacker Tactics,” December 18, 2001, http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics (accessed October 17, 2010).

[66] John Lund, “Social Networking Websites: the Next Cyber War Zone?,” April 29, 2010, http://medillnsj.org/04/2010/medill-reporting/covering-conflicts/social-networking-websites-the-next-cyber-war-zone (accessed October 17, 2010).

[67] Barak H. Obama, National Security Strategy, (Washington, DC: The White House, May 2010), 27.

[68] U.S. Joint Chiefs of Staff, Joint Publication 3-0: Joint Operations (Washington: U.S. Joint Chiefs of Staff, September 19, 2006), I-7.

[69] U.S. Congress, Senate, U.S.-China Economic and Security Review Commission, *China's Military Modernization and it's Impact on the United States and the Asia-Pacific*: *Hearing Before the U.S.-China Economic and Security Review Commission,* 110th Cong., 1st sess., March 29-30, 2007, 8.

[70] Rick Yannuzzi, "In-Q-Tel: A New Partnership Between the CIA and the Private Sector," May 4, 2007, linked from the U.S. Central Intelligence Agency website at https://www.cia.gov/library/publications/additional-publications/in-q-tel/index.html#copy (accessed December 12, 2010).

[71] Ibid.

[72] The United States Marine Corps, "Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPERNET," August 3, 2009, http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx (accessed October 17, 2010).

[73] Deputy Secretary of Defense, "Directive-Type Memorandum (DTM) 09-26 – Responsible and Effective Use of Internet-based Capabilities," February 25, 2010, http://www.defense.gov /NEWS/DTM%2009-026.pdf (accessed October 17, 2010).

[74] Brian Knowlton, "Military Claims Possible Russian Cyber Attack From Thumb Drive," August 25, 2010, http://www.infowars.com/military-claims-possible-russian-cyber-attack-from-thumb-drive (accessed October 17, 2010).

[75] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27-28.

[76] Matthew Bobby, "DoD-DHS Memorandum of Understanding Aims to Improve Cybersecurity Collaboration," November 15, 2010, linked from the Harvard National Security Journal at http://www.harvardnsj.com/2010/11/dod-dhs-memorandum-of-understanding-aims-to-improve-cybersecurity-collaboration (accessed December 12, 2010).

[77] Al Jazzerra, "YouTube Removes 'al-Qaeda Videos," November 4, 2010, http://english.aljazeera.net/news/Americas/2010/11/2010114204058597893.html (accessed December 12, 2010).

[78] Ibid.

[79] Gartner, Inc., http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp (accessed March 14, 2011).